**HHS Incident Report**

HHS Information Security and Privacy Office (ISPO)

All security and privacy incidents, including lost or stolen equipment, must be reported to a supervisor immediately. The supervisor must document the incident on this form and submit it to your appointed **HHS liaison\***.

|  |  |
| --- | --- |
| Current Date | Date and Time (if known) the Incident Occurred: |
|       | Date      | Time      |
| Date the Incident was Discovered      | Type of Lost or Stolen Equipment      |
| HHS Division/Bureau(CSRU, ACFS, MHDS, IME, etc.)      | HHS Contractor      | HHS Contract Manager      |

|  |
| --- |
| **Incident Reporter** |
| Name      | Title      |
| Work Telephone      | Mobile Telephone      |
| Email      |
| Work Address      |

|  |
| --- |
| **State or Contract Staff Involved in the Incident** (Attach additional pages if more than one.) |
| Name      | Title      |
| Work Telephone      | Email      |
| Work Address      |
| Was the supervisor of the staff involved notified? [ ]  Yes [ ]  No |
| Was law enforcement notified? [ ]  Yes [ ]  No |

|  |
| --- |
| **Type of Incident** (Check the box of all that apply.) |
| [ ]  Virus/malicious code | [ ]  Unauthorized software | [ ]  Denial of service attack |
| [ ]  Unauthorized access | [ ]  Unauthorized physical access | [ ]  User account compromised |
| [ ]  Unauthorized disclosure | [ ]  Lost or stolen equipment | [ ]  Other:       |

|  |
| --- |
| **Type of Data Involved** (Check the box of all that apply.) |
| [ ]  Federal Tax Information (FTI) | [ ]  Social Security Administration (SSA) |
| [ ]  Protected Health Information (PHI)If PHI, are any affected individuals dually eligible for Medicaid and Medicare?[ ]  Yes [ ]  No | [ ]  Personally Identifiable Information (PII) |
| Specify specific dually eligible individuals in “Description of the Incident” section below. |

|  |
| --- |
| **Type of Computer or Media Affected** (Check the box of all that apply.) |
| [ ]  Desktop computer | [ ]  Laptop/tablet | [ ]  Server |
| [ ]  Paper document | [ ]  Portable media (flashdrive, DVD, etc.) | [ ]  Mobile phone |
| [ ]  Electronic data |  |  |
| Was the data encrypted? | [ ]  Yes [ ]  No |
| Other information available:       |

|  |
| --- |
| **Description of the Incident** |
|       |

|  |
| --- |
| **Description of How the Incident Was Discovered** |
|       |

|  |
| --- |
| **Risk Mitigation** |
| Please confirm any of the following attestations you received from the unauthorized recipient. 1. Originals were destroyed, returned or deleted. [ ]  2. No copies were made. [ ]  3. Information was not further disseminated. [ ]  |
| If you left any of the three checkboxes above blank, explain what happened.      |

|  |
| --- |
| **Incident Assessment** |
| Was this incident a threat to a critical agency/facility service? [ ]  Yes [ ]  No |
| Was this incident a threat to a client’s confidentiality? [ ]  Yes [ ]  No |
| How many individuals are impacted?       |
| Are any of these impacted individuals minors? [ ]  Yes [ ]  No |
| If the number of individuals impacted is over 500, does the incidentimpact more than 500 individuals who live in the same state? [ ]  Yes [ ]  No |

|  |
| --- |
| **Data Elements Involved in the Incident** (Check the box of all that apply.) |
|  **1. Iowa Code § 217.30 and 42 CFR §431.305** |
| [ ]  Names and addresses of individuals receiving services or assistance from the Department or Medicaid Managed Care, and the types of services or amounts of assistance provided |
| [ ]  Information concerning the social or economic conditions or circumstances of particular individuals who are now receiving or have received services or assistance from the Department or Medicaid Managed Care |
| [ ]  Evaluations of personal information about a particular individual |
| [ ]  Medical or psychiatric data, including diagnosis and past history of disease or disability, concerning a particular individual |
| [ ]  Social security number of a particular individual |
| [ ]  Medical services provided regarding a particular individual |
| [ ]  Details of the types of services or amounts of assistance provided to a particular individual |
| [ ]  Information received for verifying income eligibility and amount of medical assistance payments regarding a particular individual |
|  **2. Iowa Code Chapters 228, 229** |
| [ ]  Information concerning an individual’s mental health |
| **3. Iowa Code § 141A.9** |
| [ ]  Information regarding diagnosis or treatment of HIV or AIDS |
| **4. 42 CFR pt. 2 and Iowa Code § 125.37** |
| [ ]  Information regarding treatment of substance abuse |
| **5. Iowa Code Chapter 715C** |
| First name or first initial and last name, in combination with any one or more of the following: |
| [ ]  Driver’s license number or other unique identification number created or collected by a government body |
| [ ]  Unique biometric data such as a fingerprint, retina, iris image or other unique physical representation of biometric data |
| [ ]  Social security number |
| [ ]  Unique electronic identifier or routing code, financial account, credit card or debit card number in combination with a required security code, access code or password that would permit access to an individual’s financial account |
| **6. Unique Identification Number Issued or Created that Indicates Health Care Coverage is or was Previously Provided** |
| [ ]  Issued or created by government agency (also see Iowa Code Chapter 715C) |
| [ ]  Issued or created by a business associate of HHS |
| **7. HIPAA Regulations** |
| [ ]  Information that was created or received by HHS or a business associate that is covered by HIPAA regulations that relates to care provided, physical or mental status, or eligibility for a health care program of an identifiable individual or with which you reasonably believe could be used to identify the individual |
| **8. Miscellaneous** |
| [ ]  Child abuse information, assessment or reports |

|  |
| --- |
| **Actions Taken to Date** |
| What actions have been taken to mitigate any damage to the impacted individual or to protect against further breaches?      |

The assigned **HHS liaison\*** must immediately email this form to ISPO at: DHS, Incidents.

For further information on incident response, see the current version of the following documents located on the DHS ISPO SharePoint site at the following link: [DHS Security Policies](http://dhssp/ddm/spo/_layouts/viewlsts.aspx)

* Incident Response Policy
* Incident Response Procedures
* Incident Response Team Activation Plan

|  |
| --- |
| **For ISPO Use Only:** |
| Date Incident Report Received at ISPO:      | The following documents are saved in the ISPO Incidents share as appropriate:[ ]  Incident Report[ ]  Risk Analysis[ ]  Document/Information Involved[ ]  Breach Notification Letter[ ]  Other:       |
| ISPO Spreadsheet Incident Number:      |
| Date Incident Report Submitted to HHS/OCR:      [ ]  NA |
| Date ISPO Closed Incident Report:      |

\* HHS employee that serves as the liaison between a business associate, contractor or a HHS division/bureau and the ISPO.